(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
29. Juli 2004 (29.07.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/064316 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32

(21) Internationales Aktenzeichen: PCT/DE2003/004190

(22) Internationales Anmeldedatum:
19. Dezember 2003 (19.12.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 01 100.5 8. Januar 2003 (08.01.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **TRINKEL, Marian** [DE/DE]; Waschpöl 14b, 52372 Kreuzau OT Untermaubach (DE).

(74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente) PA10, Am Kavalleriesand 3, 64295 Darmstadt (DE).

(81) Bestimmungsstaaten *(national)*: JP, US.

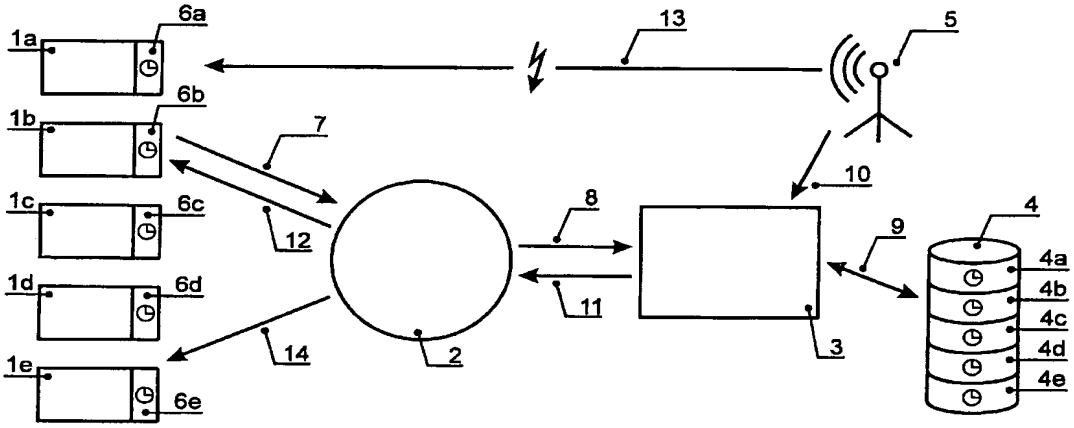
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: TELECOMMUNICATION-ASSISTED TIME STAMP

(54) Bezeichnung: TELEKOMMUNIKATIONSGESTÜTZTER ZEITSTEMPEL



(57) **Abstract:** The invention relates to a method and system for providing a time stamp by means of a manipulation-proof time signal (5, 10) via a telecommunication network (2), wherein a network subscriber (1a, 1b, ..., 1e) requests an especially officially recognized time signal (5,10) from an especially certified central system (3). Said signal is encrypted by the central system (3) using at least one key, is transmitted to the network subscribers (1a, 1b, ..., 1e) via the telecommunication network (2) after encryption and is decrypted by the subscribers using the same key(s). The invention also relates to a method for transmitting data with a manipulation-proof time stamp.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Verfahren und ein System zur Bereitstellung eines Zeitstempels durch ein manipulationssicheres Zeitsignal (5, 10) über ein Telekommunikationsnetzwerk (2), bei dem ein Netzwerkteilnehmer (1a, 1b, ..., 1e) von einem insbesondere zertifizierten Zentralsystem (3) ein insbesondere amtlich anerkanntes Zeitsignal (5, 10) anfordert, welches vom Zentralsystem (3) mit wenigstens einem Schlüssel verschlüsselt wird, nach der Verschlüsselung über das Telekommunikationsnetzwerk (2) an den Netzwerkteilnehmer (1a, 1b, ..., 1e) übermittelt und von diesem mit demselben/denselben Schlüssel/n entschlüsselt wird. Die Erfindung betrifft weiterhin ein Verfahren zur Übermittlung von Daten mit einem manipulationssicheren Zeitstempel.

WO 2004/064316 A1

Telekommunikationsgestützter Zeitstempel

Die Erfindung betrifft ein Verfahren zur Bereitstellung eines Zeitstempels durch ein manipulationssicheres Zeitsignal über ein Telekommunikationsnetzwerk sowie ein zugehöriges System zur Erzeugung eines manipulationssicheren Zeitstempels in netzwerkbasierten Kommunikationssystemen und ein Verfahren zur Übermittlung von Daten mit einem manipulationssicheren Zeitstempel über ein Telekommunikationsnetzwerk von einem ersten Netzwerkteilnehmer zu einem zweiten Netzwerkteilnehmer.

Die Problematik eines sicheren elektronischen Zeitstempels tritt überall dort in Anwendungen auf, wo die Zeit der Erstellung von Daten oder Dokumenten und/oder der Zugang solcher elektronischer Daten zeitlich nachgewiesen werden muss. Insbesondere durch die elektronische Verbreitung von Post, beispielsweise in Form von e-mails, voice mails, Faxe etc. wird ein gesicherter Zeitstempel unentbehrlich, zumal bei digitalen Signaturen eine manipulationsgesicherte Zeitangabe erforderlich ist.

Grundsätzlich ist es denkbar ein Zeitsignal, welches zur elektronischen Zeitstempelung von Daten verwendet werden soll, beispielsweise aus einem gesetzlich bzw. amtlich anerkannten Zeitzeichengeber abzuleiten. Ein solches Zeitzeichen wird in Deutschland beispielsweise über den DCF-77-Langwellensender in Braunschweig ausgestrahlt. Zwar ist dieses Zeitzeichen hochgenau, jedoch nicht manipulationssicher, so dass sich die Möglichkeit ergibt die gesendete Zeit zu manipulieren, wodurch es zu Abweichungen zwischen der tatsächlichen Zeit und der in einem elektronischen Dokument angegebenen Zeit kommen kann. Missbrauchsmöglichkeiten sind dementsprechend überall dort gegeben, wo aus wirtschaftlicher und gesetzlicher Sicht Zeitstempel zu beachten sind.

Aus der DE 198 45 198 ist es bereits bekannt ein Verfahren zur Übermittlung offizieller amtlicher Zeitinformationen bereitzustellen, bei dem eine Zeitinformation in die Netze eines Mobilnetzbetreibers eingespeist wird. Gemäß dem hier bekannten Verfahren wird die Zeitinformation von dem Mobilnetzbetreiber verschlüsselt und sodann zu einem Endgerätebetreiber, der die Entschlüsselung der Zeitinformation im Endgerät vornimmt, über das Mobilnetz übertragen. Hierbei ergibt sich eine sichere Übertragung, jeweils basierend auf der Technologie des Netzbetreibers lediglich für den Zeitraum bei der Übertragung vom Mobilnetzbetreiber zum Endgerätebetreiber. Eine Manipulationssicherheit kann jedoch nicht garantiert werden für die Zeiträume bis zum Zugang der Zeitinformation beim Mobilnetzbetreiber, so dass hier insbesondere durch die offenen Vermittlungsstellen in Kommunikationsnetzwerken Missbrauchsmöglichkeiten gegeben sind.

Aufgabe der Erfindung ist es ein manipulationssicheres telekommunikationsbasiertes Verfahren und System für die Bereitstellung eines Zeitstempels zu schaffen, welches eine deutlich höhere Sicherheitsstufe im Vergleich zum Stand der Technik aufweist.

Diese Aufgabe wird gemäß der Erfindung dadurch gelöst, dass ein Netzwerkteilnehmer von einem insbesondere zertifizierten Zentralsystem ein Zeitsignal anfordert, wobei es sich bei diesem Zeitsignal bevorzugt um ein amtlich anerkanntes Zeitsignal, wie z.B. das des DCF 77-Senders handelt. Dieses Zeitsignal wird bereits vor der Einspeisung in ein Telekommunikationsnetzwerk von dem bevorzugt zertifizierten Zentralsystem mit wenigstens einem Schlüssel verschlüsselt und erst nach dieser Verschlüsselung in ein Telekommunikationsnetzwerk eingespeist und über dieses an den Netzwerkteilnehmer übermittelt. Dieser ist sodann in der Lage das verschlüsselte Datenpaket mit demselben oder denselben Schlüsseln zu entschlüsseln und so ein manipulationsgesichertes Zeitsignal zu empfangen.

Gegenüber dem bekannten Verfahren im Stand der Technik hat das erfindungsgemäße Verfahren bereits den Vorteil, dass das amtlich anerkannte Zeitsignal bereits vor der Einschleusung in ein Kommunikationsnetzwerk von einem bevorzugt zertifizierten Zentralsystem, welches beispielsweise in einem sogenannten Trust-Center ausgebildet ist, zu verschlüsseln. Dieses Zentralsystem bietet mit seinen erhöhten Sicherheitsanforderungen eine höhere Sicherheitsstufe als das im Stand der Technik beschriebene Verfahren, da hier die für Manipulationen besonders anfälligen Vermittlungsstellen aufgrund der vorverlagerten Verschlüsselung keine Angriffspunkte mehr bilden können.

Die eigentliche Verschlüsselung und Entschlüsselung des Zeitsignales sowohl beim Zentralsystem als auch beim Netzwerkteilnehmer kann über dem einschlägigen Fachmann hinlänglich bekannte Verschlüsselungsalgorithmen vollzogen werden, die wenigstens einen Schlüssel zur Verschlüsselung der Information benötigen. Die Art der Verschlüsselung, beispielsweise durch digitale Signaturen, Hashfunktionen etc. liegen im Belieben des Fachmannes.

Wie zuvor beschrieben, ist es für die vorgesehene Verschlüsselung bei dem Zentralsystem und der nachfolgenden Entschlüsselung des Zeitzeichens beim Netzwerkteilnehmer nötig, dass sowohl das Zentralsystem als auch der Netzwerkteilnehmer im Besitz desselben Schlüssels bzw. derselben Schlüssel sind. Da hier grundsätzlicher Art wiederum die Möglichkeit zur Manipulation besteht, nämlich dadurch, dass ein über längere Zeit verwendeter Schlüssel ausspioniert werden kann, ist es in einer bevorzugten Weiterbildung vorgesehen, dass sich wenigstens ein Schlüssel, der sowohl beim Zentralsystem als auch beim Netzwerkteilnehmer hinterlegt ist, synchron bei beiden Hinterlegungsstellen ändert, insbesondere nach vorgegebenen Zeitintervallen. Damit ist dieser Schlüssel jeweils immer bei beiden Hinterlegungsstellen zu gleichen Zeiten identisch vorhanden, ändert sich jedoch bevorzugt in kurzen Zeitintervallen von z.B. lediglich wenigen Sekunden, so dass die Möglichkeit zum Ausspionieren eines solchen Schlüssels nachhaltig herabgesetzt wird. Das erfindungsgemäße Verfahren wird

dementsprechend mit einem zeitlich variablen Schlüssel ausgeführt, der beim Netzwerkteilnehmer und beim Zentralsystem identisch vorliegt. Von einem solchen Schlüssel können grundsätzlich auch mehrere vorliegen und in dem genannten Verfahren verwendet werden.

Die zeitlich synchrone Änderung dieses Schlüssels beim Netzwerkteilnehmer und beim Zentralsystem wird bevorzugt dadurch erreicht, dass sowohl beim Netzwerkteilnehmer als auch beim Zentralsystem je wenigstens ein Uhrsystem vorgesehen ist, wobei das Uhrsystem beim Netzwerkteilnehmer einem Uhrsystem beim Zentralsystem zugeordnet ist und beide Uhrsysteme wiederum ihrerseits einem konkreten Netzwerkteilnehmer zugeordnet sind. Diese beiden Uhrsysteme arbeiten zeitlich synchron und sind dafür vorgesehen einen zeitlich sich ändernden Schlüssel beim Netzwerkteilnehmer und dem Zentralsystem wie zuvor beschrieben zu erzeugen, so dass dieser sich zeitlich synchron ändernde Schlüssel zur Verschlüsselung und Übertragung des Zeitsignales verwendet werden kann. Gegebenenfalls können auch mehrere Uhrsysteme eingesetzt werden, um mehrere Schlüssel zu erzeugen.

Hier kann es vorgesehen sein, dass die beiden Uhrsysteme hardwaremäßig ausgebildet sind und von dem insbesondere zertifizierten Zentralsystem nach der Anmeldung eines Netzwerkteilnehmers ausgegeben werden. Das Zentralsystem wird nach der Anmeldung eines Netzwerkteilnehmers zu dem erfindungsgemäßen Verfahren zwei Uhrsysteme zeitlich miteinander synchronisieren, eines bei sich behalten und eines dem Netzwerkteilnehmer z.B. käuflich oder als Leihgabe zur Verfügung stellen. Hierdurch ist die absolute Synchronität der beiden Uhrsysteme und die Identität des Schlüssels bei beiden Hinterlegungsstellen zu gleichen Zeiten gegeben.

Gemäß dem erfindungsgemäßen Verfahren wird es nötig sein, verschiedene Uhrsysteme, die entsprechend unterschiedlichen Netzwerkteilnehmern zugeordnet sind, untereinander zu unterscheiden. Hierfür ist es gemäß der Erfindung

bevorzugt vorgesehen, dass das Zentralsystem bei der Abfrage eines Zeitsignales durch einen Netzwerkteilnehmer ein diesem zugeordnetes und beim Zentralsystem vorliegendes Uhrsystem anhand einer übermittelten Kennung ermittelt. Bei dieser Kennung kann es sich z.B. um eine solche handeln, die den Netzwerkteilnehmer innerhalb des Kommunikationsnetzwerkes eindeutig identifiziert. In beispielsweise kabelgebundenen Telefonnetzen kann es sich hierbei z.B. um die sogenannte Call-Line-Identity (CLI) handeln, in Mobilfunknetzen um das sogenannte Home Location Register (HLR), im Internet um die sogenannte IP-Adresse oder in anderen Systemen um eine Kennung umfassend PIN- und PAN-Nummern, die ebenfalls zur eindeutigen Identifizierung herangezogen werden können.

Die Eindeutigkeit ergibt sich im Wesentlichen schon dadurch, dass jede Zuordnung der Kennungen lediglich erst nach einer persönlichen Identifizierung des Besitzers z.B. durch einen Personalausweis herausgegeben wird. So beispielsweise die CLI bei der Anmeldung eines Telefonanschlusses, das HLR bei der Unterzeichnung eines Mobilfunkvertrages und die IP-Adresse im Internet bei der Registrierung bei einem Internetprovider, der selbst bei dynamischer Adressvergebung zumindest die providerinterne Kennung registriert.

Mittels einer solchen, von dem Netzwerkteilnehmer bei der Abfrage des Zeitsignales zur Verfügung gestellten Kennung ergibt sich dementsprechend die Möglichkeit beim Zentralsystem das diesem Netzwerkteilnehmer eindeutig zugeordnete Uhrsystem zu ermitteln, aus diesem Uhrsystem den erzeugten Schlüssel zur Verschlüsselung des Zeitsignales zu verwenden und anschließend das verschlüsselte Zeitsignal über das Telekommunikationsnetzwerk an den Netzwerkteilnehmer zu versenden.

Alternativ kann es vorgesehen sein, das Zeitsignal unabhängig von einem durch ein Uhrsystem erzeugten Schlüssel lediglich alleine durch die zusätzlich zur Verfügung gestellte Kennung des Netzwerkteilnehmers zu verschlüsseln oder in einer Weiterbildung der Erfindung sowohl den durch das Uhrsystem erzeugten

Schlüssel als auch die übermittelte Kennung gleichzeitig und/oder nacheinander zur Verschlüsselung heranzuziehen.

Das oben genannte Verfahren hat neben der Tatsache einer manipulationssicheren Zeitsignalübermittlung weiterhin den Vorteil, dass eine Ortsreferenz des Netzwerkteilnehmers gegeben ist, die sich durch die zur Verfügung gestellte Kennung, also beispielsweise die CLI, das HLR oder ähnliches ergibt. Diese Ortskennung oder aber auch weitere Identifikation des abfragenden Netzwerkteilnehmers trägt zu einer weiteren Erhöhung der Sicherheitsstufe bei, da schon alleine diese Kennungen schwer manipulierbar sind.

Nach einer Abfrage und Übermittlung des Zeitsignales von dem beschriebenen Zentralsystem liegt dementsprechend gemäß dem erfindungsgemäßen Verfahren bei dem Netzwerkteilnehmer ein manipulationsgesichertes, insbesondere zertifiziertes Zeitsignal vor, welches zur Zeitstempelung z.B. von Daten, die über das Telekommunikationsnetzwerk übermittelt werden sollen, herangezogen werden können. Ebenso ist das so erhaltene Zeitsignal für sämtliche Arten der Zeitstempelung einsetzbar, selbst wenn keine weitere Übermittlung der Daten vorgesehen ist.

So ist es beispielsweise möglich, dass ein Netzwerkteilnehmer in dem Augenblick, wo er über ein Telekommunikationsnetzwerk Daten von Seiten Dritter empfängt den zeitlichen Eingang dieser Daten durch einen Zeitstempel registriert, wobei der Zeitstempel gemäß dem oben beschriebenen Verfahren von einem Zentralsystem erhalten wird. Hierfür braucht der Netzwerkteilnehmer nach Erhalt der Daten lediglich bei dem zertifizierten Zentralsystem das Zeitsignal über das Netzwerk anfordern.

Ebenso kann es in einer Weiterbildung des oben genannten Verfahrens vorgesehen sein, dieses Verfahren auch zur Übermittlung von Daten mit einem manipulationssicheren Zeitstempel über ein Telekommunikationsnetzwerk von

einem ersten Netzwerkteilnehmer zu einem zweiten Netzwerkteilnehmer heranzuziehen.

Dies kann bevorzugt dadurch erfolgen, dass die Daten, die von einem ersten Netzwerkteilnehmer zusammen mit einem Zeitsignal als Zeitstempel, welches gemäß dem zuvor beschriebenen Verfahren erhalten wird, an einen zweiten Netzwerkteilnehmer direkt oder indirekt über das Zentralsystem übermittelt werden.

So kann es nach dem Erhalt des Zeitsignales von dem Zentralsystem vorgesehen sein, dass die zu übermittelnden Daten und/oder das Zeitsignal bei der Übermittlung vom absendenden ersten Netzwerkteilnehmer verschlüsselt werden. Die Verschlüsselung kann sich gemäß der Erfindung sowohl auf die Daten oder das Zeitsignal alleine beschränken, als auch eine Verschlüsselung sowohl der Daten als auch des Zeitsignales gleichzeitig erfolgen. Besonders bevorzugt wird für die verschlüsselte Übermittlung der Daten an den zweiten Netzwerkteilnehmer der Schlüssel verwendet, der sowohl beim Netzwerkteilnehmer als auch beim Zentralsystem zeitlich synchron vorliegt. Alternativ wird eine Verschlüsselung mittels der Kennung des Netzwerkteilnehmers erfolgen bzw. in einer bevorzugten Ausführung eine Verschlüsselung mit beiden Möglichkeiten, also sowohl dem Schlüssel als auch der Kennung gleichzeitig oder nacheinander.

Erfindungsgemäß kann es vorgesehen sein, dass bei einer indirekten Übermittlung der Daten über das Zentralsystem das Zentralsystem die Daten an den zweiten empfangenden Netzwerkteilnehmer weiterleitet und dieser sicher sein kann, dass die Daten beim Zentralsystem zum zertifizierten Zeitpunkt angekommen sind. Dies kann als Zugangskontrolle der Daten eingesetzt werden, sofern der Netzwerkteilnehmer, der die Daten erhalten soll, sich dem Zentralsystem angeschlossen hat. Auch für diese Weiterleitung können sich Zentralsystem und der empfangende Teilnehmer des erfindungsgemäßen Verfahrens bedienen.

Alternativ ist es vorgesehen, dass ein zertifiziertes Zentralsystem direkt bei einem Netzwerkteilnehmer vorgesehen ist, wenn dieser Netzwerkteilnehmer den zeitlichen Zugang von Daten nachweisen muss. Dies kann z.B. regelmäßig bei Ämtern und Behörden der Fall sein, beispielsweise bei Patentämtern, wo der Eingang der Dokumente gemäß dem heutigen Stand der Technik in den Papierdokumenten durch eine Lochstempelung erfolgt. Eine elektronische Stempelung von elektronischen Dokumenten kann hingegen mit dem erfindungsgemäßen Verfahren durchgeführt werden. Ebenso ist der Einsatz bei Finanzämtern und anderen Behörden gegeben.

Bevorzugt wird sich eine entsprechende Behörde oder ein entsprechendes Amt, welches einen Nachweis über den zeitlichen Zugang von elektronischen Dokumenten führen muss, selbst eines zertifizierten Zentralsystemes bedienen und eine Zeitstempelung mit dem oben beschriebenen Verfahren zulassen.

Zur weiteren Absicherung kann es vorgesehen sein, dass das Zentralsystem eine Empfangsquittierung ausstellt, so dass der erste absendende Kommunikationsteilnehmer eine Rückmeldung darüber erhält, dass das Dokument mit seinem Zeitstempel beim Empfänger angekommen ist. Für die Empfangsquittung selbst kann beispielsweise wieder das Zeitsignal mit dem oben beschriebenen Verfahren übermittelt werden oder die Quittierung erfolgt über eine andere Art der Datenübertragung.

Mit dem oben beschriebenen Verfahren kann die Manipulationsfreiheit einer Dokumentensendung auf einfache Art und Weise überprüft werden, da beispielsweise nach der Übermittlung des Zeitsignales auf Anforderung eines ersten Telekommunikationsteilnehmers bei diesem Teilnehmer das manipulationsfreie, sicher übertragende Zeitsignal vorliegt, wobei dieses Zeitsignal den Absendezeitpunkt des Zeitstempels bei dem Zentralsystem repräsentiert.

Unter der Voraussetzung genügend kurzer Datenlaufzeiten wird der Netzwerkteilnehmer mit seinem synchron laufenden Uhrsystem im Idealfall denselben Schlüssel verwenden, um das übermittelte Zeitsignal wieder zu entschlüsseln. Sollte aufgrund einer zeitlichen Intervallüberschreitung das Uhrsystem beim Netzwerkteilnehmer bereits weiter gelaufen und einen nächsten Schlüssel generiert haben, wird der Netzwerkteilnehmer mit seinem Verschlüsselungssystem feststellen, dass sich keine sinnvolle Zeit aus dem erhaltenen Datenpaket entschlüsseln lässt und gegebenenfalls auf einen bevorzugt abgespeicherten vorherigen Schlüssel des Uhrsystemes zurückgreifen. Sollte sich auch mit diesem vorherigen Schlüssel keine sinnvolle Zeit entschlüsseln lassen, so erfolgt ein weiterer Rückgriff auf den wiederum vorherigen Schlüssel und sofort, bis dass eine maximal tolerierbare Signallaufzeitüberschreitung festgestellt wird, welches den erhaltenen Zeitschlüssel als ungültig erscheinen lässt, so dass gegebenenfalls ein neuer Zeitschlüssel angefordert wird.

Bei einer erfolgreichen Decodierung des Zeitsignales wird dieses wie oben erwähnt z.B. zur Zeitstempelung empfangener Daten und/oder zur Versendung der Daten an einen Empfänger verwendet und durch den vom Uhrsystem neu generierten Schlüssel verschlüsselt und im folgenden an das Zentralsystem entweder eines Empfängers oder zur Weiterleitung an einen Empfänger übersandt, bei dem mit demselben zuvor beschriebenen Verfahren die Entschlüsselung innerhalb eines tolerierbaren Zeitintervalles erfolgt. Sollte die Entschlüsselung erfolglos sein, bedeutet dies, dass entweder an dem übermittelten Datenpaket eine Manipulation stattgefunden hat oder dass eine maximal tolerierbare Datenlaufzeit überschritten wurde.

Es kann somit mit dem erfindungsgemäßen Verfahren sichergestellt werden, dass zu übermittelnde Daten zu einem bestimmten Zeitpunkt abgesendet wurden, wobei dieser Zeitpunkt dem Zeitsignal entspricht, welches von dem Zentralsystem zur Verfügung gestellt wurde. Gegebenenfalls kann von dem Empfänger im Kommunikationsnetzwerk nach der Entschlüsselung des Absendezeitpunktes eine

Datensendung als fristgemäß anerkannt werden, wenn eine eventuelle sehr lange Datenlaufzeit nicht in das Verschulden des Absenders fällt.

Die oben beschriebenen Verfahren können bevorzugt durch ein System zur Erzeugung eines manipulationssicheren Zeitstempels in netzwerkbasierten Kommunikationssystemen realisiert werden, bei dem das System ein Zentralsystem und je ein Uhrsystem auf Seiten eines Netzwerkteilnehmers und des Zentralsystemes umfasst, wobei die Uhrsysteme einander und einem Netzwerkteilnehmer zugeordnet sind und synchron arbeiten zur Erzeugung eines sich insbesondere in Zeitintervallen ändernden Schlüssels. Mittels dieses Schlüssels kann ein insbesondere amtlich anerkanntes Zeitsignal in dem Zentralsystem verschlüsselt und nach Übersendung an einen Netzwerkteilnehmer von diesem entschlüsselt werden, so dass diesem Netzwerkteilnehmer ein manipulationsgesicherter Zeitstempel zur Verfügung steht.

Ein Ausführungsbeispiel der Erfindung ist in der nachfolgenden Abbildung dargestellt. Die Figur 1 zeigt mehrere Netzwerkteilnehmer 1a – 1e, die über ein Telekommunikationsnetzwerk 2 untereinander in Verbindung stehen können. In Verbindung mit dem Telekommunikationsnetzwerk 2 ist weiterhin ein Zentralsystem 3 vorgesehen, welches ein manipulationssicheres Zeitsignal zur Verfügung stellen kann. Dieses manipulationssichere Zeitsignal basiert beispielsweise auf einem amtlich bzw. gesetzlich anerkannten Zeitzeichensender 5, wie z.B. in Deutschland dem DCF-77-Sender.

Grundsätzlich besteht die Möglichkeit, dass ein Telekommunikationsteilnehmer 1a auf direktem Wege 13 das Zeitzeichensignal von dem Zeitzeichensender 5 empfängt. Dieses Zeitzeichensignal ist jedoch in keinem Falle manipulationssicher, da die Erzeugung dieses Signales leicht imitiert und so falsche Zeitzeichensignale erzeugt werden können. Auch kann das amtliche Zeitzeichen nicht in allen Regionen aufgrund von Abschattung der Radiowellen empfangen werden.

Gemäß der Erfindung ist es vorgesehen, dass ein Netzwerkteilnehmer 1b über eine Kommunikationsverbindung 7 und das Netzwerk 2 sowie die Kommunikationsverbindung 8 von einem am Netzwerk 2 angeschlossenen Zentralsystem 3 ein Zeitsignal 5/10 anfordert. Hierbei übermittelt der Teilnehmer 1b automatisch eine Kennung z.B. bei einer Telefonverbindung oder über das Internet, wo sowohl die IP-Adresse als auch die kabelgebundene Telefonnummer oder Call-Line-Identity übertragen wird.

Über diese dem Zentralsystem 3 zur Verfügung gestellte Kennung kann das Zentralsystem aus einer Uhrsystem-Sammlung 4 gegbenenfalls mittels einer Datenbank das dem Netzwerkteilnehmer zugeordnete Uhrsystem 4b ermitteln und aus diesem Uhrsystem 4b einen Schlüssel auslesen, der zur Verschlüsselung des Zeitsignales, welches von dem Signalsender 5 über den Kommunikationsweg 10 zur Verfügung gestellt wird, herangezogen werden. Gegebenenfalls wird zur weiteren Verschlüsselung des Zeitsignales auch die Kennung des Netzwerkteilnehmers 1b verwendet.

Das Zentralsystem 3 sendet über den Kommunikationsweg 11, das Netzwerk 2 und den Kommunikationsweg 12 das verschlüsselte Zeitsignal an den Teilnehmer 1b, wobei dieser Teilnehmer nach Empfang des Signales mit dem von seinem eigenen Uhrsystem 6b erhaltenen synchronen Schlüssel das Zeitsignal entschlüsseln und weiter verwenden kann. Die weitere Verwendung liegt beispielsweise in einer Zeitstempelung von Daten, die der Teilnehmer anderweitig empfangen hat oder versenden möchte.

Gegenüber dem alternativen Kommunikationsweg 13, nämlich dem direkten Empfang des Zeitzeichens hat der beschriebene Weg zum Empfang des Zeitsignales den Vorteil einer wesentlich höheren Manipulationssicherheit, da bereits außerhalb des reinen Transportbereiches über das Telekommunikationsnetzwerk 2 die Verschlüsselung und Entschlüsselung des Zeitsignales erfolgt. Es kann hier gegenüber dem oben benannten Stand der

Technik dementsprechend eine eindeutige Trennung zwischen Verarbeitung und Verschlüsselung der Daten und Transport der Daten durch einen Netzbetreiber erfolgen.

Mit dem so erhaltenen Zeitsignal kann der Teilnehmer 1b entweder von einem Dritten erhaltene Daten stempeln und ablegen oder seinerseits das Zeitsignal an zu versendende Daten anfügen und erneut mit dem Schlüssel seines eigenen Uhrsystemes 6b verschlüsseln und dem Zentralsystem 3 zusenden, welches bei einem Empfänger installiert ist oder die Daten z.B. an einen ebenfalls dem Verfahren angeschlossenen Netzwerkteilnehmer 1e über die Kommunikationsverbindung 11, das Netz 2 und die Verbindung 14 zusenden.

Das Zentralsystem 3 muss für einen manipulationssicheren Transport des Zeitsignales seinerseits lediglich dafür Sorge tragen, dass es selbst das Zeitsignal, z.B. von einem amtlich anerkannten Sender, z.B. DCF-77, unverfälscht erhält. Dies kann bevorzugt dann der Fall sein, wenn der Zeitzeichensignalgeber, beispielsweise der DCF-77-Sender, seinerseits die Aufgabe des zertifizierten Zentralsystemes übernimmt, so dass praktisch keine Kommunikationswege für ein unverschlüsseltes Zeitsignal existieren.

Andererseits ist es möglich, dass jegliches Amt oder Behörde, welches einen zeitlichen Empfang quittieren muss, sich auf ein internes Uhrsignal zurückzieht und dieses Uhrsignal Telekommunikationsteilnehmern als zumindest amtsintern anerkannte Referenz zusendet.

Bezugszeichenliste

1a - 1e	Netzwerkteilnehmer
2	Telekommunikationsnetzwerk
3	Zentralsystem
4	Uhrsystem-Sammlung
4a – 4e	Uhrsysteme
5	Zeitsignal
6a – 6e	Uhrsysteme
7 - 14	Kommunikationsverbindungen/ Kommunikationswege

Patentansprüche

1. Verfahren zur Bereitstellung eines Zeitstempels durch ein manipulationssicheres Zeitsignal (5, 10) über ein Telekommunikationsnetzwerk (2), **dadurch gekennzeichnet, dass** ein Netzwerkteilnehmer (1a, 1b, ..., 1e) von einem insbesondere zertifizierten Zentralsystem (3) ein insbesondere amtlich anerkanntes Zeitsignal (5, 10) anfordert, welches vom Zentralsystem (3) mit wenigstens einem Schlüssel verschlüsselt wird, nach der Verschlüsselung über das Telekommunikationsnetzwerk (2) an den Netzwerkteilnehmer (1a, 1b, ..., 1e) übermittelt und von diesem mit demselben/denselben Schlüssel/n entschlüsselt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** sich wenigstens ein Schlüssel, der sowohl beim Netzwerkteilnehmer (1a, 1b, ..., 1e) als auch bei einem Zentralsystem (3) vorliegt, synchron beim Netzwerkteilnehmer und beim Zentralsystem ändert, insbesondere nach vorgegebenen Zeitintervallen.

3. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** beim Netzwerkteilnehmer (1a, 1b, ..., 1e) und beim Zentralsystem (3) je wenigstens ein Uhrsystem (4a, 4b, ..., 4e, 6a, 6b,..., 6e) vorgesehen ist, wobei je zwei Uhrsysteme (4a - 6a, 4b - 6b,..., 4e - 6e) einander und dem Netzwerkteilnehmer (1a, 1b, ..., 1e) zugeordnet sind und synchron arbeiten zur Erzeugung eines sich zeitlich synchron ändernden Schlüssels.

4. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** das Zentralsystem (3) bei der Abfrage eines Zeitsignales (5,10) durch einen Netzwerkteilnehmer (1a, 1b, ..., 1e) ein diesem zugeordnetes Uhrsystem (4a, 4b, ..., 4e) anhand einer übermittelten Kennung, insbesondere der Netzwerkadresse des Netzwerkteilnehmers (1a, 1b, ..., 1e), ermittelt und mittels einem von dem zugeordneten Uhrsystem

(4a, 4b, ..., 4e) erzeugten Schlüssel und/oder der Kennung das Zeitsignal (5,10) verschlüsselt und übersendet.

5. Verfahren zur Übermittlung von Daten mit einem manipulationssicheren Zeitstempel über ein Telekommunikationsnetzwerk (2) von einem ersten Netzwerkteilnehmer zu einem zweiten Netzwerkteilnehmer **dadurch gekennzeichnet, dass** die Daten von dem ersten Netzwerkteilnehmer zusammen mit einem Zeitsignal, welches gemäß einem Verfahren nach einem der vorherigen Ansprüche erhalten wurde, an den zweiten Netzwerkteilnehmer direkt oder indirekt über das Zentralsystem (3) übermittelt werden.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** die Daten und/oder das Zeitsignal bei der Übermittlung vom ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) verschlüsselt werden, insbesondere mit dem beim Zentralsystem (3) und ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) vorliegenden Schlüssel und/oder einer Kennung des ersten Netzwerkteilnehmers (1a, 1b, ..., 1e) .

7. Verfahren nach einem der Ansprüche 5 bis 6, **dadurch gekennzeichnet, dass** ein Zentralsystem (3) beim zweiten Netzwerkteilnehmer vorgesehen ist.

8. Verfahren nach einem der Ansprüche 5 bis 7, **dadurch gekennzeichnet, dass** das Zentralsystem (3) eine Empfangsquittierung, insbesondere mit einem Zeitsignal (5,10) an den ersten Netzwerkteilnehmer (1a, 1b, ..., 1e) zurücksendet.

9. System zur Erzeugung eines manipulationssicheren Zeitstempels in netzwerkbasierten Kommunikationssystemen **dadurch gekennzeichnet, dass** es ein Zentralsystem (3) und je ein Uhrsystem (4a, 4b, ..., 4e, 6a, 6b,..., 6e) auf seiten eines Netzwerkteilnehmers (1a, 1b, ..., 1e) und des Zentralsystems (3) umfasst, wobei die Uhrsysteme (4a - 6a, 4b - 6b,..., 4e - 6e) einander und dem Netzwerkteilnehmer (1a, 1b, ..., 1e) zugeordnet sind

und synchron arbeiten zur Erzeugung eines sich insbesondere in Zeitintervallen ändernden Schlüssels mittels dem ein insbesondere amtlich anerkanntes Zeitsignal (5,10) im Zentralsystem (3) verschlüsselbar und nach Übersendung an den Netzwerkteilnehmer (1a, 1b, ..., 1e) von diesem entschlüsselbar ist.

10. System nach Anspruch 9, **dadurch gekennzeichnet, dass** ein Zeitzeichensender (5) das Zentralsystem (3) bildet.

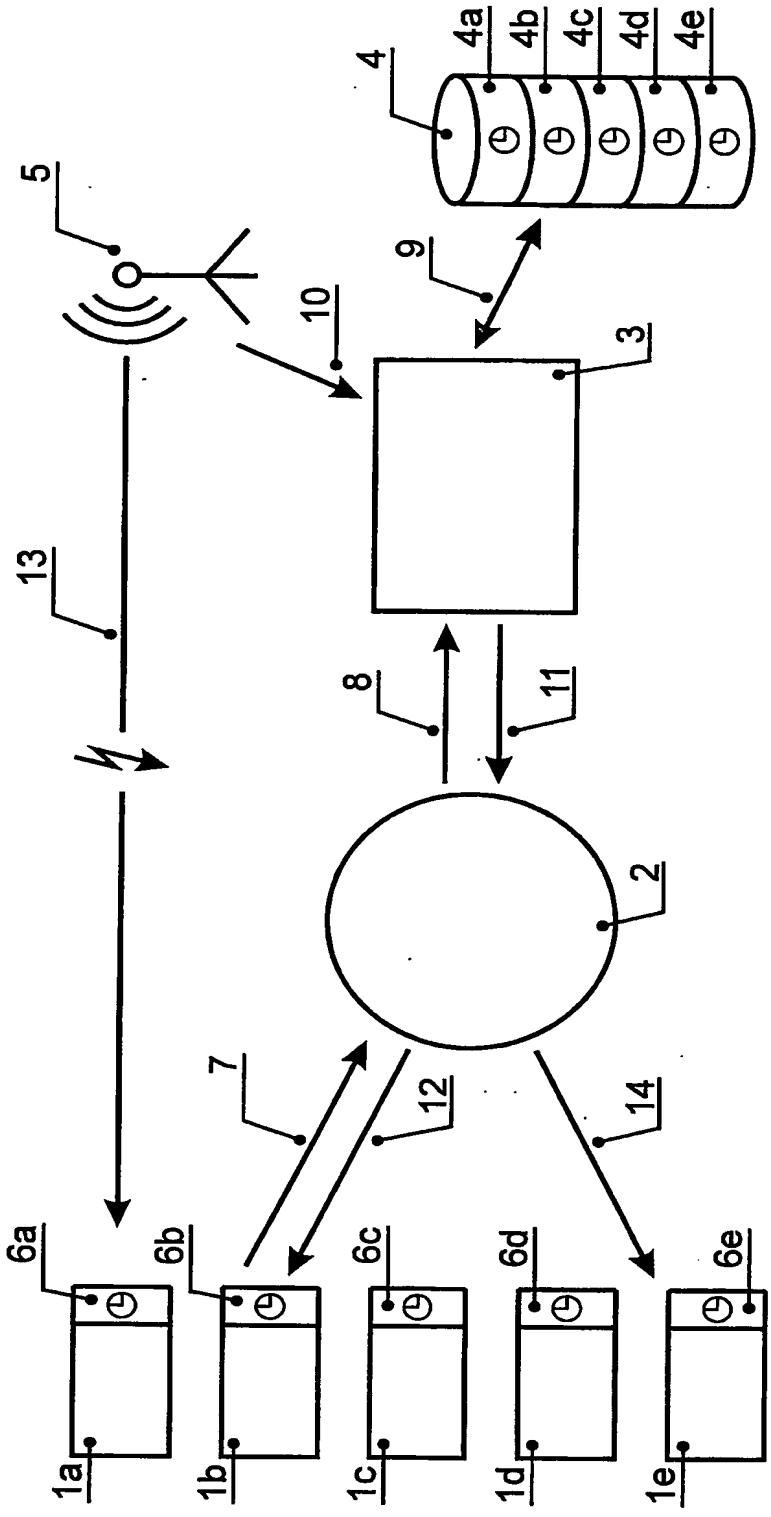


Fig. 1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 03/04190

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G04G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	DE 198 45 199 A (MAZ MIKROELEKTRONIK ANWENDUNGS) 6 April 2000 (2000-04-06) page 3, line 8 - line 16 page 3, line 33 - line 41 page 3, line 45 - line 55; claim 1	1,2,5-8 3,4,9,10
Y A	US 2002/169970 A1 (CANDELORE BRANT L) 14 November 2002 (2002-11-14) paragraphs '0008!,'0034!,'0036!,'0040!,'0044!,'0046!; claims 23-25; figures 1,3	1,2,5-8 3,4,9,10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 2004	19/04/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Cretaine, P

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 03/04190

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19845199 A	06-04-2000	DE 19845199 A1	06-04-2000
US 2002169970 A1	14-11-2002	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/DE 03/04190

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L G04G

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y A	DE 198 45 199 A (MAZ MIKROELEKTRONIK ANWENDUNGS) 6. April 2000 (2000-04-06) Seite 3, Zeile 8 - Zeile 16 Seite 3, Zeile 33 - Zeile 41 Seite 3, Zeile 45 - Zeile 55; Anspruch 1	1,2,5-8 3,4,9,10
Y A	US 2002/169970 A1 (CANDELORE BRANT L) 14. November 2002 (2002-11-14) Absätze '0008!,'0034!,'0036!,'0040!,'0044!,'0046!; Ansprüche 23-25; Abbildungen 1,3	1,2,5-8 3,4,9,10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
6. April 2004	19/04/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cretaine, P

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 03/04190

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19845199 A	06-04-2000	DE 19845199 A1	06-04-2000
US 2002169970 A1	14-11-2002	KEINE	